

## Definitions

### (To be added to Glossary)

1. **Crypto-asset:** Crypto-asset, within the context of the CBB Rulebook, Volume 6 and Module CRA: Crypto-asset, refers to virtual or digital assets or tokens operating on a blockchain platform and protected by cryptography. Tokens are broadly of four types: Payment tokens, Utility tokens, Asset tokens and Hybrid tokens.
  - i. **Payment tokens (Exchange tokens):** Payment tokens (synonymous with cryptocurrencies) are virtual currencies which are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. Payment tokens give rise to no claims on their issuer and are usually decentralised. The most prominent example is Bitcoin.
  - ii. **Utility tokens:** Utility tokens are tokens that are intended to provide access to a specific application or service but are not accepted as a means of payment for other applications.
  - iii. **Asset tokens:** Asset tokens represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, these tokens are analogous to equities, bonds or derivatives. Tokens which enable physical assets to be traded on the blockchain also fall into this category.
  - iv. **Hybrid Tokens:** Hybrid tokens are those that have features of one or more of the other three types of tokens.
2. **Virtual Currency** is a digital representation of value that can be digitally traded and function as: (i) a medium of exchange; and/or (ii) a unit of account; and/or (iii) a store of value, but does not have legal tender status. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (real currency, real money or national currency), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is digital representation of fiat currency used to electronically transfer value denominated in fiat currency.
3. **Accepted Crypto-asset:** means a payment token (cryptocurrency) permitted by the CBB for the purpose of undertaking the regulated crypto-asset service by a crypto-asset licensee.
4. **Fiat Currency:** means government issued currency that is designated as legal tender in its country of issuance through government decree, regulation or law.

5. **Regulated crypto-asset services:** Any of the regulated activities permitted to be undertaken by a crypto-asset licensee as outlined in Module CRA Paragraph CRA-1.1.6.
6. **Crypto-asset licensee:** is a person licensed by the CBB under the Crypto-asset Module of Rulebook 6.
7. **Crypto-asset license:** a license issued by the CBB under the crypto-asset Module of Rulebook Volume 6
8. **Crypto-asset exchange:** means a center or network established for the purpose of trading or exchanging of crypto-assets, which operates by matching orders in the normal course of business.
9. **Overseas crypto-asset service licensee:** A crypto-asset licensee incorporated in an overseas jurisdiction but licensed to operate within the Kingdom of Bahrain.
10. **Appointed Expert(s):** A duly qualified individual or firm appointed by the CBB to carry out inspections in accordance with Article 114 of the CBB Law or special investigations of licensees in accordance with Article 121 of the CBB Law. Appointed experts may be appointed in addition to the CBB's own officials. Examples of appointed experts include reporting accountants, lawyers, private investigators, expert witnesses and independent actuaries.
11. **Trilateral Meetings:** A meeting between a licensee, an appointed expert and the CBB.
12. **Qualified by Exception:** A report issued by an appointed expert that is qualified and indicates that certain areas or issues remain unresolved or are unverifiable due to certain limitations imposed on the appointed experts' work. The report will clearly indicate the type and reason for exception and the action taken by the appointed experts had the mentioned limitation not been placed on their work.
13. **Cyber Security Incident:** means an observable occurrence indicating a possible breach in the systems, network and operating environment.
14. **Cyber Security Risk Resilience:** means the ability to anticipate, absorb, adapt to, rapidly respond to, and recover from disruption caused by a cyber-attack.
15. **Cyber Security Risk:** means the combination of the probability of an incident occurring within the realm of a licensee's information assets, systems and operating environment.
16. **Cyber Security Threat:** means a circumstance or incident with the potential to intentionally or unintentionally exploit one or more vulnerabilities in a licensee's information assets, systems and operating environment.
17. **Information Assets:** means any piece of data, device or other component of the environment that supports information-related activities.

18. **Malware:** means malicious software used to disrupt the normal operation of an information system in a manner that adversely impacts its confidentiality, integrity or availability.
19. **Recovery Time Objective (RTO):** means targeted duration of time which an information system and network must be recovered after a cyber breach.